Click Here & Upgrade
Expanded Features
Unlimited Pages
PDF Complete Documents

# COMMITTEE ON GOVERNMENT REFORM

**TOM DAVIS, CHAIRMAN**

## *MEDIA ADVISORY*

**For Immediate Release**
**April 5, 2005**

**Contact: Robert White/Drew Crockett**
**(202) 225-5074**

# Leave No Computer System Behind:

*Committee to Examine Federal Government's*
*D+ Grade for Information Security*

**What:** **Government Reform Committee Oversight Hearing: "No Computer System Left Behind: A Review of the Federal Government's D+ Information Security Grade"**

**When:** **THURSDAY, APRIL 7, 2005, 10:00 A.M.**

**Where:** **ROOM 2154, RAYBURN HOUSE OFFICE BUILDING**

**Background:**

Our economy and government have become more and more dependent on information technology and the Internet. Government agencies have improved the efficiency of their operations and services to citizens through electronic government initiatives. Given the interconnectivity of systems, all it takes is one weak link to break the chain. Cyber attacks are evolving and becoming more sophisticated; they may originate from criminals, terrorists, and hostile nations.

Having a strong IT security management framework is key to ensuring the federal government has the ability to respond to the emerging cyber threats. A government information security management program must be comprehensive, yet flexible enough to adapt to the changing cyber threat environment. Chairman Tom Davis wrote the Federal Information Security Management Act (FISMA) to provide that kind of framework. Therefore, compliance with the Act is critical to protect our economy and national security. The FISMA reports submitted to Congress by the agency Chief Information Officers (CIOs) and the Inspectors General (IGs) are used to compile the Committee's annual scorecards, which help us gauge government information security progress.

Click Here & Upgrade
Expanded Features
Unlimited Pages
PDF Complete Documents

While the grade for government agencies overall rose 2.5 points last year, the grade itself is only a D+. Some agencies showed marked improvement in their security management practices, while others maintained a poor standard of performance. This year's scorecard process highlights some challenges in the evaluation and reporting processes that the Committee will examine. The grades are a helpful way for Congress to gauge an agency's progress, but this is by no means an exact science. The Committee will also explore the reasons some agencies continue to under-perform.

Panel One witnesses will focus on information security from a government-wide perspective. Panel Two is comprised of agency representatives and will focus on the agency-level perspective on FISMA implementation. Both panels will address whether agencies need additional guidance, procedures, or resources to improve their information security and fully comply with FISMA. The process provides agencies with a strong management framework, but it is not a panacea; there may be a need for amendments to facilitate implementation of the security concepts that drive FISMA.

## WITNESSES

**Panel One:**

**Greg Wilshusen**, Director, Information Security Issues, Government Accountability Office

**Karen S. Evans**, Administrator, Office of E-Government and Information Technology, Office of Management and Budget

**Panel Two:**

**Bruce N. Crandlemire**, Assistant Inspector General for Audit, US Agency for International Development

**John Streufert**, Acting Chief Information Officer, US Agency for International Development

**Frank Deffer**, Assistant Inspector General for Information Technology, Department of Homeland Security

**Steve Cooper**, Chief Information Officer, Department of Homeland Security

**Ted Alves**, Assistant Inspector General for IT and Financial Management, Department of Transportation

**Daniel Matthews**, Chief Information Officer, Department of Transportation

###